REMARKS

The foregoing amendment amends the specification and Claims 1, 2, 7 and 10-12 to correct clerical errors. Claims 1-12 are pending in this application. For the reasons set forth below, Applicants believe that the rejections should be withdrawn and that Claims 1-12 are in condition for allowance.

REJECTION OF CLAIMS 1-12 UNDER 35 U.S.C. 102(e)

The Examiner rejected Claims 1-12 under 35 U.S.C. 102(e) as being anticipated by U.S. Patent No. 6,996,724 to Murakami *et al.* ("Murakami"). As discussed below, this rejection is respectfully traversed.

Claim 1

Claim 1 requires generating the random number partial data from a random number in correspondence to the original partial data, generating the divided partial data by using exclusive OR ("XOR") calculation of the original partial data and the random number partial data, and generating the divided data in the desired number of divisions from the divided partial data.

According to one embodiment of the invention, the random number partial data R(j) is generated from a random number in correspondence to the original partial data S(j), the divided partial data D(i, j) are generated by using XOR calculation of the original partial data S(j) and the random number partial data R(j), and then as many divided data D(i) as the desired number of divisions (n) are generated from the divided partial data D(i, j).

The original partial data S(j) are obtained by simply partitioning the original data S by the prescribed processing unit bit length. Thus the original data S can be reconstructed by simply concatenating the original partial data S(j). However, the divided data D(i) are n sets of data that are not obtained by partitioning the original data S, so the original data S cannot be reconstructed by simply concatenating the divided data D(i).

The divided data D(i) can be reconstructed by concatenating the divided partial data D(i, j), and the divided partial data D(i, j) are obtained by using XOR calculation of the original partial data S(j) and the random number partial data R(j). As illustrated in Figure 3

and described in the specification, event though there is an XOR calculation used to obtain the divided partial data D(i, j), the calculation requires more than simply taking an XOR value of the original partial data S(j) and the random number partial data R(j).

Murakami discloses a method for generating a secret key of an entity in ID-NIKS (ID-based non-interactive key sharing scheme). Murakami teaches that an ID vector Ia (identification information such as name, address, etc.) of entity a is divided into a plurality of ID division vectors Iaj (j=1, 2 … J). Then the j-th center extracts a row vector, which corresponds to the ID division vector of entity a, from the symmetric matrix Hj and carries out an XOR on all of the components of the extracted row vector with an individual random α a(j) so as to be generated as a secret key vector Saj. *See*, Col. 6, ll. 25 – Col. 7, ll. 25; Col. 7, ll. 34 - Col. 8, ll. 19; Figs. 2-4.

Claim 1 recites, "generating the divided data in the desired number of divisions from the plurality of divided partial data, such that the original data cannot be ascertained from any one divided data alone but the original data can be recovered from a prescribed number of the divided data among generated divided data." According to one embodiment, the divided data D(i) and the divided partial data D(i, j) are defined such that the original data S can be recovered from a prescribed number of the divided data D(i) but not from any one divided data D(i) alone.

Murakami does not disclose or suggest the divided data and the divided partial data, such that the divided data can be obtained by constructing the divided partial data, and the original data can be recovered from a prescribed number of the divided data but not from any one divided data alone, as required by Claim 1. None of the figures and corresponding sections of Murakami, as cited by the Examiner, show otherwise. Accordingly, Claim 1 is patentable over Murakami.

Claims 2-10

Claims 2-10 depend from Claim 1. Accordingly, for at least the same reasons discussed above, Claims 2-10 are patentable over Murakami.

Moreover, with regard to Claim 2, Murakami does not disclose or suggest that the original partial data and the random number partial data are generated as many as the desired number of divisions minus one, as required by Claim 2.

With regard to Claim 3, Murakami fails to disclose or suggest that the divided data includes one or more divided data formed by a random number alone, and one or more divided data formed by the divided partial data generated by the XOR calculation of one or more original partial data and one or more random number partial data, as required by Claim 3.

With regard to Claim 6, Murakami does not teach or suggest that the divided data include two or more divided data formed by the divided partial data generated by the XOR calculation of one or more original partial data and one or more random number partial data, as required by Claim 6.

Claim 7 defines a specific method of generating divided partial data, where each divided partial data D(i,j) is generated by:

$$D(i,j) = S(j) * \left\{ \prod_{k=1}^{n-1} Q(j,i,k) \right\}$$

when $i < n$, and D(i,j) is generated by:

$$D(i,j) = R(j)$$

when $i = n$, while changing variable i from 1 to n and variable j from 1 to n-1 for each variable i. Claim 7 further defines that when $i < n$ that:

$$\prod_{k=1}^{n-1} Q(j,i,k) = Q(j,i,1)*Q(j,i,2)* \cdots *Q(j,i,n-1)$$

where "*" denotes the XOR calculation. *See*, Lines 20-30 of Claim 7. None of the figures and corresponding sections of Murakami, as cited by the Examiner, teach or suggest any particular method of calculating each divided partial data. More specifically, Murakami does not teach or suggest the specific method of generating each divided partial data, as recited by Claim 7.

With regard to Claim 8, Murakami does not disclose or suggest that each divided data is generated such that a random number component cannot be eliminated by carrying out calculation among the divided partial data that constitutes the each divided data, as required by Claim 8.

None of the figures and corresponding sections of Murakami, as cited by the Examiner, show otherwise. Accordingly, Claims 2-10 are patentable over Murakami.

Claims 11 and 12

Claims 11 and 12 recite similar elements as Claim 1. Accordingly, for at least the same reasons discussed above, Claims 11 and 12 are patentable over Murakami.

CONCLUSION

The foregoing is submitted as a complete response to the Office Action identified above. This application should now be in condition for allowance, and the Applicants solicit a notice to that effect. If there are any issues that can be addressed via telephone, the Examiner is asked to contact the undersigned at 404.532.6946.

Respectfully submitted,

/Elizabeth V. Thomas/

By: Elizabeth V. Thomas
Reg. No. 63,509

KILPATRICK STOCKTON LLP
1100 Peachtree Street, Suite 2800
Atlanta, Georgia 30309-4530
Telephone: (404) 815-6500
Facsimile: (404) 815-6555
Docket No. 44471/317116